BİLGİ GÜVENLİĞİ
DERNEĞİ

17. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı

ISC TÜRKİYE2024

ISCTÜRKİYE 2024 SONUÇ BİLDİRGESİ

23 EKİM 2024

ISCTÜRKİYE 2024 SONUÇ BİLDİRGESİ

17. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı-ISC Türkiye 2024, ‘Siber Dayanıklılık ve Olgunluk’’ ana temasıyla, 16-17 Ekim 2024 tarihlerinde T.C. Cumhurbaşkanlığı Millet Kütüphanesi’nde gerçekleştirilmiştir. Bilgi Güvenliği Derneği tarafından düzenlenen Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi himayelerinde; Gazi Üniversitesi, İstanbul Teknik Üniversitesi, Orta Doğu Teknik Üniversitesi, TOBB Ekonomi ve Teknoloji Üniversitesi işbirliği ile gerçekleştirilmekte, Ulaştırma ve Altyapı Bakanlığı, Sanayi ve Teknoloji Bakanlığı, Cumhurbaşkanlığı Savunma Sanayi Başkanlığı, Bilgi Teknolojileri ve İletişim Kurumu, IEEE Türkiye ve “Avrupa Ağ ve Siber Güvenlik Ajansı-ENISA” tarafından desteklenmektedir.

Konferansa, Türk Keneşi Aksakallılar Konseyi Başkanı ve son Başbakan Sn. Binali YILDIRIM, Ulaştırma ve Altyapı Bakanı Sn. Abdulkadir URALOĞLU, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanı Sn. Yusuf TANCAN, Orta Doğu Teknik Üniversitesi Rektörü Sn. Prof. Dr. Ahmet YOZGATLIGİL, TOBB ETÜ Rektörü Sn. Prof. Dr. Yusuf SARINAY, kamuda kurumlarından genel müdürler, daire başkanları, akademisyenler, siber güvenlik ve bilişim uzmanları, başta olmak üzere 1500’ün üzerinde kişi online ortamda kayıt yaptırmış ve 1200’in üzerinde katılım olmuştur.

Konferans, Millet Kütüphanesi ana salonda şehitlerimiz için Saygı Duruşu ve İstiklal Marşımızın okunmasıyla başlamış, BGD Yönetim Kurulu Başkanı Prof. Dr. Mustafa ALKAN’ın açılış konuşması akabinde, Konferans Akademik Başkanı Doç. Dr. Oğuz YAYLA’nın konuşması sonrasında, TOBB ETÜ Rektörü Sn. Prof. Dr. Yusuf SARINAY ve Orta Doğu Teknik Üniversitesi Rektörü Sn. Prof. Dr. Ahmet YOZGATLIGİL hocaların konuşmalarını müteakiben, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanı Yusuf TANCAN konuşmasını yapmış ve daha sonra Ulaştırma ve Altyapı Bakanı Sn. Abdulkadir URALOĞLU ve son olarak da Türk Keneşi Aksakallılar Konseyi Başkanı ve son T.C. 27. Dönem Başbakanı Sn. Binali YILDIRIM konuşmasını yapmıştır.

Açılış konuşmaları hemen sonrasında,

- **Sayın Binali YILDIRIM,**
- **UAB Haberleşme Genel Müdürlüğü**
- **Ulusal Siber Olaylara Müdahale Merkezi**
- **ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi Programı**

- **Dr. Ali Taha KOÇ**
- **İhlas Haber Ajansı**
- **Picus Security**
- **Siber Anadolu Toplulukları**

olmak üzere 8 dalda "BGD Siber Güvenlik Üstün Hizmet Ödülleri" verilmiştir.

Bilgi Güvenliği Derneği "**SİBER GÜVENLİK ÜSTÜN HİZMET ÖDÜLLERİ"** belirli kriterler temel alınarak BGD Yönetim Kurulu tarafından belirlenmekte ve her yıl verilmektedir. Bu temel kriterler şunlardır;
- Teknik ve Bilimsel Katkılar ile Yenilikçilik
- Eğitim, Bilinçlendirme ve Farkındalık Faaliyetleri
- Siber Vatan Savunmasına Fikir,Altyapı,Organizasyon,Ürün ve Hizmetler
- Siber Güvenlik Ekosisteminin Oluşturulması ve Geliştirilmesine Katkılar
- Profesyonel Kariyer ve Liderlik ile Nitelikli Uzman Yetiştirme
- Güvenlik Açıkları, Riskleri ve Tehditlerin Tespiti ve Giderilmesi
- Yasal Düzenlemelere ve Ulusal Strateji ve Eylem Planına Katkılar
- Etik ve Toplumsal Sorumluluk
- İş Birliği ve Paylaşım Kültürü Oluşturma ve Yaygınlaştırma
- Ulusal ve Uluslararası Ödüller, Standartlar, Sertifikasyon ve Uyumluluk

Ödüller; kişi**, kurum**, sektör, **üniversite,** medya ve **özel ödül** olmak üzere 6 kategoride verilmektedir. Ödüller ve gerekçeleri aşağıda verilmiştir.

Sayın Binali YILDIRIM; Türk Keneşi Aksakallılar Konseyi Başkanı, Son Başbakanımız, Meclis Başkanımız, Bakanımız ve Milletvekilimiz bugüne kadar ülke bilgi güvenliği ve savunmasının gelişmesine vermiş olduğu önemli katkılar, Bilgi Güvenliği Derneği olarak ön hazırlığını yaptığımız ulusal siber güvenlik stratejisi ve eylem planı taslak çalışma önerimizi destekleyip ilk siber güvenlik ulusal stratejisi ve eylem planı çalışmalarını UAB liderliğinde başlatması, Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi Yönetilmesi ve Koordinasyonunu Bakanlar Kurulu adına yürütmesi, bilgi güvenliği derneğinin düzenlediği bilgi güvenliği ve kriptoloji konferansı gibi ulusal ve uluslararası etkinliklere bizzat katılarak desteklemesi ve bizleri yapacağımız çalışmalarda sürekli yüreklendirmesi ve en önemlisi de gerek kamuoyunda gerekse kurumlarda bilgi güvenliği farkındalığının oluşması, güvenlik altyapılarının kurulması ve siber vatanımızın güvenliğinin sağlanmasına olan katkılarından dolayı sayın vekilimiz, bakanımız ve başbakanımız Sayın **Binali YILDIRIM Bey**'e **"Bilgi Güvenliği Derneği Siber Güvenlik Üstün Hizmet Ödülü"** verilmiştir.

UAB Haberleşme Genel Müdürlüğü; ülkemizde ilk Ulusal Siber Güvenlik Stratejisi ve Eylem Planlarının hazırlanması, yayımlanması ve koordinasyonu,

Ulusal planların ve yapılan faaliyetlerin takip edilmesi, ülkemizin 2024-2028 yıllarını kapsayan siber güvenlik alanında vizyonunu ortaya koyan strateji ve eylem planının güncellenerek yayımlanmasına sunduğu katkılardan dolayı **Ulaştırma ve Altyapı Bakanlığı Haberleşme Genel Müdürlüğüne "Bilgi Güvenliği Derneği Siber Güvenlik Üstün Hizmet Ödülü"** verilmiştir.

Ulusal Siber Olaylara Müdahale Merkezi; ülkemizde siber güvenlik stratejisi ve eylem planı kapsamında BTK bünyesinde kurulan bir birim olması, ülkemizin siber güvenliği ve savunmasına bugüne kadar yapmış olduğu çok önemli katkıları, ulusal tehdit oluşturan saldırıların engellenmesi ve ortadan kaldırılması, AVCI, AZAD, *KASIRGA,* ATMACA, SINKHOLE, KULE, **SOME İletişim Portalı** gibi pek çok yerli ve milli çözümler geliştirmesi, SOME altyapılarını kurması ve yönetmesi ile ulusal siber güvenlik risklerinin giderilmesine sunduğu katkılardan dolayı Ulusal Siber Olaylara Müdahale Merkezi kısava **USOM**'a **"Bilgi Güvenliği Derneği Siber Güvenlik Üstün Hizmet Ödülü"** verilmiştir.

ODTÜ Uyg. Matematik Enst. Kriptografi Programı; ülkemizde Kriptoloji biliminin gelişmesi, yüzlerce nitelikli uzman yetiştirmesi ve ileri düzey çalışmalara imza atması, kriptografik test modülü ve sistem güvenliği laboratuvarlarını kurulmasına öncülük etmesi, kriptoloji alanında en çok tez yaptıran program olması, düzenlediği etkinlikler ile kriptoloji alanında ülke bilgi birikiminin artmasına olan katkıları, akademik bilgi birikimini sektöre ve kurumlara aktarması ve en önemlisi ise bu konferansımızın kriptoloji bölümünün ilk günden beri destekçisi ve isim babası olmalarından dolayı **ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi Programına "Bilgi Güvenliği Derneği Siber Güvenlik Üstün Hizmet Ödülü"** verilmiştir.

Dr. Ali Taha KOÇ; Cumhurbaşkanlığı Dijital Dönüşüm Ofisi bünyesinde siber güvenlik dairesi başkanlığının kurulması, ülke siber güvenlik stratejisi ve eylem planının güncellenmesi, Bilgi ve İletişim Güvenliği Denetim *Rehberinin hazırlanması ve yayınlanması,* Türkiye Siber Güvenlik Kümelenmesi Platformu faaliyetlerinin Savunma Sanayii Başkanlığı ile birlikte yürütülmesi, siber güvenlik liselerinin kurulmasına öncülük etmesi, güvenlik ve kriptoloji alanında yapılan bilimsel çalışmaları desteklemesi ve en önemlisi gençlerin siber güvenliğe olan ilgilerinin artırılmasına katkılarından dolayı Dr. Ali Taha KOÇ'a **"Bilgi Güvenliği Derneği Siber Güvenlik Üstün Hizmet Ödülü"** verilmiştir.

İHLAS HABER AJANSI; ülkemizde bilgi güvenliği ve kriptoloji alanında toplumu bilgilendiren haberlere yer vermesi, toplumun bilgi güvenliği alanında farkındalığının arttırılmasına katkı sağlaması, özellikle de bilgi güvenliği

uzmanlarının görüşlerine haberlerinde yer vermesinden dolayı **İhlas Haber Ajansına "Bilgi Güvenliği Derneği Siber Güvenlik Üstün Hizmet Ödülü"**verilmiştir.

PICUS SECURITY; Otomatik Sızma Testi, Siber İhlal ve Saldırı Simülasyonu ile Saldırı Tespit Kuralı Doğrulama yeteneklerini aynı platformda bir araya getiren ilk ve tek Ofansif Güvenlik Doğrulama çözümü sunması, ülkemizde siber güvenliğinin gelişmesine yapmış olduğu öncül katkılar, geliştirmiş olduğu ürünler, yurtiçi ve yurtdışındaki başarıları, DMO'nun kataloğunda ürünlerinin bulunması, dünya çapında 50'den fazla ülkede 500'den fazla kurumsal müşterisinin olması, son dönemde ise 80 milyon dolar yatırım alıp dünya çapında bir başarı hikayesine sahip olmasından dolayı **Picus Security**'e **"Bilgi Güvenliği Derneği Siber Güvenlik Üstün Hizmet Ödülü"** verilmiştir.

SIBER ANADOLU TOPLULUKLARI; Üniversite gençliğinin siber güvenliğe olan ilgisinin artırılması ve üniversitelerde pek çok siber güvenlik öğrenci topluluğunu bir çatı altında toplayarak bir araya getirmeleri, işbirliği ve güç birliği yapmaları, öğrenciler arasında siber güvenlik bilincinin davranışa dönüştürülmesi ve yaygınlaştırılma çabaları, verdikleri eğitimler, yaptıkları yarışmalar ve en önemlisi ise siber güvenlik alanına gençlerin ilgisini artırdıkları için **Siber Anadolu Topluluklarına "Bilgi Güvenliği Derneği Siber Güvenlik Üstün Hizmet Ödülü"** verilmiştir.

Ödül töreni sonrasında, Konferansa Platin, Altın, Gümüş, Yaka ve Stant Sponsoru olarak destek veren 19 firmaya plaketleri, Sayın YILDIRIM ve Sayın URALOĞLU tarafından verilmiştir.

Açılış konuşmaları ve Ödül Törenine ait videolara buradan erişilebilir.

Çay ve kahve arası sonrasında, "Haberleşmede Siber Dayanıklılık" başlıklı oturum başlamış, bu oturumda, Türksat Genel Müdürü Ahmet Hamdi ATALAY, Turkcell Şebeke Teknolojilerinden Sorumlu Genel Müdür Yardımcısı Prof. Dr. Vehbi Çağrı GÜNGÖR, Türk Telekom Genel Müdür Yrd. Ali TAŞKIN, Vodafone Türkiye İcra Kurulu Başkan Yardımcısı Özlem KESTİOĞLU konuşmalarını yapmıştır.

Bu oturuma ilişkin videoya buradan erişilebilir.

Daha sonra, "Siber Dayanıklılık Ve Olgunluk" birinci oturumu gerçekleştirilmiş, bu oturumda, Milli İstihbarat Akademisi Başkanı Prof. Dr. Talha KÖSE, UAB Haberleşme Genel Müdür Yardımcısı Onur GENÇER, ASELSAN Genel Müdür Yardımcısı Mustafa YAMAN, STM Siber Güvenlik ve Bilişim Sistemleri

Direktörü Bülent ARSAL, Vodafone Türkiye Kurumsal Teknoloji Çözümleri Direktörü Burcu ALTINTAŞ konuşmalarını yapmıştır.

Bu oturuma ilişkin videoya buradan erişilebilir.

Öğle arası sonrasında, "Siber Dayanıklılık ve Olgunluk" ikinci oturumu gerçekleştirilmiş, bu oturumda, Ankara Kalkınma Ajansı Genel Sekreteri Av. Dr. Duhan KALKAN, Huawei Türkiye Cyber Security and Privacy Officer Boran DEMİRCİLER, Kıta Bilişim Alan Danışmanı E. Tuğg. Halil İbrahim BÜYÜKBAŞ, Havelsan Siber Güvenlik Direktörü Salih TALAY konuşmalarını yapmıştır.

Bu oturuma ilişkin videoya buradan erişilebilir.

Akabinde, **Davetli Konuşmacı/Keynote Speaker olarak,** Bilkent Üniversitesi öğretim üyesi Prof. Dr. Serdar KOZAT, "Büyük Dil Modelleri İle Genel Yapay Zekâya Büyük Adım / Big Step from LLM to Artificial General Intelligence" başlıklı konuşmasını yapmıştır.

Davetli konuşmacının konuşmasına ilişkin videoya buradan erişilebilir.

"Dijital Hizmetlerde Siber Güvenlik Ve Kimlik Doğrulama" başlıklı oturumda, Hazine ve Maliye Bakanlığı, Bilgi Teknolojileri Genel Müdürü Dr. Mert ÖZARAR, MEB Yenilik ve Eğitim Teknolojileri Genel Müdürü Mustafa CANLI, Türksat Siber Güvenlik Yönetimi Direktörü Mehmet Ali ERKUL, BiOnay Genel Müdür Yardımcısı Nusret Atilla BİLER konuşmalarını yapmıştır.

Bu oturuma ilişkin videoya buradan erişilebilir.

Konferansın 2. gününde akademik oturumlarda 17 makale "Siber Güvenlik ve Tehdit Tespiti", "Sistem Güvenliği ve Tasarım", "Kriptografi", "Makine Öğrenmesi ve Yapay Zekâ Uygulamaları" olmak üzere 4 farklı oturumda akademisyenler tarafından sunulmuştur.

Akadmeik oturumlara paralel olarak; BGD Genç Başkanı Oğuzhan ALKAN başkanlığında Öğrenci Projeleri Sunum Oturumu gerçekleştirilmiştir. Oturumda;

- Blokzincir Tabanlı Akademik Makale Yayınlama Platformu
- Yapay Zekâ Destekli Blokzincir İstihbarat Aracı
- Akıllı Şebekeler için Zeki Siber Güvenlik Çözümleri Geliştirme: Yapay Zekâ Destekli Saldırı Tespit Sistemi Geliştirme
- Yapay Zekâ ile Tehdit İstihbarat ve Savunma
- Büyük Dil Modelleri ile Siber Güvenlik Farkındalığını Artırma

Başlıklı Projeler, 10 farklı üniversiteden katılan öğrenciler ve proje danışmanı hocalar tarafından sunulmuştur.

Proje sunumlarından sonra BGD Genç Başkanı Oğuzhan ALKAN başkanlığında, "BGD GENÇ OTURUMU" gerçekleştirilmiş, bu oturumda Siber Anadolu Toplulukları ve ODTÜ Siber Güvenlik Topluluğu Başkanı Şakir ŞİMŞEK, TED Üniversitesi Siber Güvenlik Topluluğu Başkanı Fatih PURTAŞ, Gazi Üniversitesi Siber Güvenlik Topluluğu Başkanı Elif Nur MERCAN, Gazi Üniversitesi Siber Güvenlik Araştırma ve Geliştirme Topluluğu Başkanı Tolga DEMİREL, TOBB ETÜ Siber Güvenlik Topluluğu Başkanı Alperen Tolga KARAÇAM, Ankara Yıldırım Beyazıt Üniversitesi Siber Güvenlik Topluluğu Başkanı Bilge KELEŞ konuşmalarını yapmışlar, yaptıkları etkinlikleri, gerçekleştirdikleri projelerini ve gelecek hedeflerini katılımcılar ile paylaşmışlardır.

Son olarak, "Eğitim Oturumu"nda, USOM Güvenlik Testleri Ekip Lideri Hacı Özdemir, "USOM Ulusal Faaliyetleri"; Havelsan Siber Güvenlik Uzmanı Ata Seren ise, "Siber Güvenlikte Yapay Zeka" başlıklı eğitimler vermişlerdir.

Konferans, Konferans Akademik ve Bilim Kurulu adına Prof. Dr. Şeref SAĞIROĞLU, Prof. Dr. Oğuz YAYLA, Prof. Dr. Ali Aydın SELÇUK, Bilgi Güvenliği Derneği adına Genel Sekreter Oğuz YILMAZ, Yönetim Kurulu Başkanı Prof. Dr. Mustafa ALKAN'ın kapanış ve değerlendirme konuşmasıyla sona ermiştir.

KONFERANS SONUÇ BİLDİRGESİ

Siber dayanıklılık ve olgunluk, bir ülkenin dijital altyapısının güvenliği, ekonomisinin korunması ve dijital geleceğinin sürdürülebilirliği için kritik öneme sahip kavramlardır. **Siber dayanıklılık**, bir sistemin siber saldırılara ve tehditlere karşı kendini koruma, toparlanma ve süreklilik kabiliyetini ifade ederken, **siber olgunluk** ise bu süreçlerin ne kadar gelişmiş ve sürdürülebilir olduğunu göstermektedir. Bu bağlamda, ülkelerin siber güvenliği dikkate alındığında yapılabilecek çalışmalar ve öneriler aşağıda sıralanmıştır:

1. Ülkemizde "Siber Dayanıklılık ve Olgunluk" konusuna önem verildiği, Ulaştırma ve Altyapı Bakanlığı tarafından hazırlanan 2024-2028 yıllarını kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planında stratejik amaçlarımız ve hedeflerimiz "**insan**", "**savunma**", "**caydırıcılık**" ve "**iş birliği**" temalarından yola çıkılarak belirlenmesinin önemli olduğu ve bu hedefe katkı sağlayacağı, 6 stratejik amaç, 18 hedef ve 61 eylem maddesinin yer almasının ve Siber Dayanıklılık, Proaktif Siber Savunma ve Caydırıcılık, İnsan Odaklı Siber Güvenlik Yaklaşımı, Teknolojinin Güvenli Kullanımı ve Siber Güvenliğe Katkısı, Siber Tehditlerle Mücadelede Yerli ve Milli Teknolojiler konusunda odaklanılmasının önemli olduğu ve hedeflenen çıktıların elde edilmesine katkılar sağlayacağı değerlendirilse

de bundan önceki stratejilerin ulusal siber güvenliğe katkısının iyi ölçülemediği, denetlenemediği veya verilen görevlerin tam olarak yapılmadığı bilinmektedir. Eylem planlarında verilen görevlerin denetlenmesi ve denetime dayalı siber güvenlik yaklaşımının sürekliliği önemli olduğundan bu konuya özel önem verilmelidir.

2. Proaktif siber savunma ve caydırıcılık çalışmaları kapsamında siber olaylara müdahale ekiplerinin yetkinlik seviyelerinin artırılması, siber risklerin ve tehditlerin tespiti ve bildirimi ile siber tehdit istihbaratı edinimi ve paylaşımına yönelik kabiliyetlerin geliştirilmesi ve artırılması için gereken önlemler alınmalıdır.
3. İnsan odaklı siber güvenlik yaklaşımı benimsenerek, farkındalık artırma çalışmalarına önem verilmeli ve bu alanda çalışan profesyonellerin yetkinlikleri artırılmalıdır. İnsan odaklı siber güvenlik yaklaşımı ile ülkemizin insan kaynağının güçlendirilmesine ve yetkinliğin artırılması konusunda daha üst düzey önlemler alınmalıdır.
4. "Sıfır güven (zero trust)" anlayışıyla tedbirlerin belirlenerek, güvenli bir siber ortamın ve dijital dönüşümün sağlanması, yeni teknolojilerin güvenliğine yönelik gereksinimlerin ve asgari güvenlik kriterlerinin değerlendirilmesi, belirlenmesi ve hayata geçirilmesi gereklidir.
5. Siber güvenlik alanında yenilikçi fikirlerin ve Ar-Ge faaliyetlerinin desteklenerek yerli ve millî siber güvenlik teknolojilerinin geliştirilmesine, siber güvenlik teknoparklarının açılması, yerli ürün kullanımının daha da yaygınlaştırılması için gereken adımlar atılmalıdır.
6. Ülkeler, bütüncül bir siber güvenlik stratejisi oluşturmalı ve bu stratejiyi güncel tutmalıdır. Strateji, hem kamu hem de özel sektör işbirliklerini içermelidir. Ayrıca, kriz anlarında hızlı müdahale edilebilecek bir **acil durum planı** ve **kriz yönetim prosedürü** bulunmalıdır.
7. Savunma, haberleşme, enerji, finans, sağlık gibi kritik altyapı sektörlerinde siber güvenlik tedbirlerinin belirlenmesi ve uygulanması noktasında, düzenlemelere ve bu düzenlemeler üzerinden gerçekleştirilen denetlemelere dayalı siber güvenlik yaklaşımları daha çok benimsenmelidir.
8. Siber olay öncesinin, olay esnasında ve sonrasında gerçekleştirilecek çalışmalar kadar önem taşıdığından hareketle, riskler ve tehditler oluşmadan önce veya erken aşamalarda iken önüne geçilmesi noktasında tedbirlerin alınması noktasında proaktif siber savunma anlayışıyla yürütülecek çalışmalar siber dayanıklılığı artıracaktır. Siber dayanıklılığın sağlanması ve artırılması için esas olan noktalardan birisi, güvenliğe yönelik risklerin belirlendiği, değerlendirildiği, risk azaltma çalışmalarının gerçekleştirildiği ve izlendiği mekanizmalar üzerine kurgulanan sektörel, kurumsal ve ulusal seviyede risk temelli analiz yaklaşımlarına daha fazla önem verilmelidir.
9. Sıfır güven mimarileri yaygınlaştırılmalıdır. Sıfır güven, her bir erişim

talebinin kimlik doğrulama gerektirmesi anlamına gelir ve siber dayanıklılığı artırmaktadır. Bu yapı, siber saldırı risklerini minimize edecek ve güvenlik açıklarının proaktif olarak izlenmesine katkı sağlayacaktır.

10. Yapay zekâ ve makine öğrenimi destekli **otomatik müdahale sistemleri geliştirilmelidir.** Bu sistemlerin saldırılara hızlı cevap vermesi, insan müdahalesi gerektirmeden tehditleri tespit etme ve önleme, kritik altyapıların çökmesini engelleyeceğinden bu konularda altyapılar kurulmalı ve işletilmelidir.
11. Siber güvenlik olgunluğunu artırmak için **Siber Güvenlik Olgunluk Modelleri** (örneğin CMMI - Cybersecurity Maturity Model) mutlaka kullanılmalıdır. Bu modeller, organizasyonların mevcut güvenlik durumunu analiz etmeye ve iyileştirme alanlarını belirlemeye imkan tanıdığından özel önem verilmelidir.
12. Siber tehdit istihbaratı, siber güvenlik olgunluğunu artırmanın temel unsurlarından biridir. **Tehdit istihbaratı paylaşımı** için hem yerel hem de uluslararası seviyede işbirlikleri geliştirilmeli ve siber tehditler hakkında gerçek zamanlı bilgi alışverişi yapılmalıdır. Özellikle Siber Küme içerisinde yer alan şirketlerin ortak bir platformda birleşerek dünya örneklerinde olduğu gibi bunu yapmaları gereklidir.
13. Siber güvenlik zafiyetlerinin tespitine, ilgili taraflara bildirimine ve güncel siber tehdit istihbaratı paylaşımına yönelik ulusal kapasitenin ve kabiliyetlerin artırılarak ulusal siber güvenliği tehdit edecek unsurların yapay zekâ ve büyük veri altyapılarıyla erken tespiti ve önlenmesi için daha çok çalışma yapılmalı, altyapılar kurulmalı ve yeni programlar açılmalı, açık olanlar desteklenmelidir.
14. Siber tehditlerden korunması noktasında, "tasarımdan itibaren güvenlik (security-by-design)" ilkesiyle, yerli ve millî ürün projelerinin oluşturulması, sertifikasyon ve akreditasyon mekanizmalarının geliştirilmesi konusunda daha kapsamlı çalışmalar yapılmalıdır.
15. DeepFake, yalan haber, kandırma ve dolandırıcılığın engellenmesi için **Yapay zekâ destekli dolandırıcılık tespit sistemleri** geliştirilmeli ve yaygınlaştırılmalıdır.
16. Siber tehditler uluslararası boyut kazandığından, ülkeler **siber güvenlik için küresel işbirliklerine** daha fazla katılmalı, **Avrupa Birliği NIS2** gibi direktiflerden ve **NATO'nun siber savunma inisiyatiflerinden** faydalanmalı ve yeni düzenleme ve standartlar mutlaka ilgili alanlarda kullanılmalıdır.
17. Ülkeler, dijital mahremiyeti korumak için kapsamlı **veri gizliliği yasaları** geliştirmektedir. Ülkemizde de yapay zekânın hızla geliştiği bir dönemde yapay zekâ güvenliği konularında çalışılmalı, yeni çözümler geliştirilmeli gerekirse de yasalaştırılmalıdır.
18. Dijital mahremiyetin korunması için **kuantum sonrası şifreleme** gibi ileri şifreleme teknolojilerine yatırım yapılmalı, altyapılar kurulmalı, mevcut

laboratuvarlar desteklenmelidir. Kuantum bilgisayarların ortaya çıkması, mevcut kriptografik yöntemleri tehdit etmektedir. Bu nedenle, **kuantum sonrası kriptografi** alanında araştırmalar hızlandırılmalı ve mevcut altyapılar bu yeni teknolojiye uyumlu hale getirilmelidir.

19. 5G ve/veya 6G ağları ve nesnelerin interneti cihazlarının hızla yaygınlaşmasıyla birlikte, bu teknolojilerin güvenliği büyük önem kazanmaktadır. **5G ağlarının güvenliği** sağlanmalı, IoT cihazlarının birbirine bağlanması sırasında güçlü kimlik doğrulama yöntemleri kullanılmalıdır.
20. Yapay zekâ sistemlerinin güvenilirliği ve şeffaflığını artırmak için **açıklanabilir yapay zekâ** teknolojileri geliştirilmelidir. Bu sayede, yapay zekâ sistemleri tarafından alınan kararlar daha iyi anlaşılır ve hatalar daha kolay tespit edilebilir ve daha dayanıklı sistemler geliştirilebilecektir.
21. Yeni dünya dış politikasında siber alanın önemi daha da artacağından, uluslararası ilişkilerin siber boyutu ele alınmalı, siber dış politikalara yönelik birimler kurulmalıdır. Siber uzay ve dijital teknolojiler konusunda dış politikamızı yönetecek, olası siber krizleri diplomasi yoluyla çözmeyi hedefleyecek, Dışişleri Bakanlığı bünyesinde bir siber "SİBER VATAN" birimi mutlaka hayata geçirilmelidir. Bu birim küresel siber standartları belirlemede Türkiye'nin liderliğini geliştirmeye odaklı olan "Dışişleri Bakanlığı Siber Uzay ve Politika Bürosu" olarak adlandırılabilir. Uluslararası Siber Uzay Güvenliği ve Uluslararası Bilgi Politikası olmak üzere iki yapısal birime ayrılarak çalışmalarını yürütebilir. Hatta bu yapı Türk devletleriyle birlikte organize edilerek; bir Siber Antlaşma Örgütü kurularak siber alanda hem ofansif hem de defansif bir kurum oluşturulabilir. Genel manada uluslararası alanda siber güvenlik politikaları savunma odaklıdır. Ancak artık ofansif yetenekler de politikalarda yer almalıdır. Ulusal siber güvenliği sağlamada ofansif yöntemlere başvurma kartı masaya konulmalıdır. Bu alanda Türkiye'nin yeni bir modele ihtiyacı olduğu aşikardır. Bu model şunları içerisinde barındırmalıdır;
    - "Siber Uzay Savunma Gücü" kurulmalıdır.
    - Bir muhabere taburu ofansif siber kuvvet olarak yapılandırılmalı ve bu yapının temel amaçları ise; Operasyon, Savunma, Saldırı, Sızma şeklinde olmalıdır.
    - "Bilim süvarileri" adıyla profesyonel programcı ve kodlayıcılardan oluşan, kimlikleri gizli, sürekli klavye başında olan, bir çok alanda faaliyet gösteren, sıcak bölgelerde ve siber savaşlarda görev yapabilecek olan gizli bir Ordu kurulmalıdır. Bu Ordu, gerçek zamanlı siber istihbarat elde etmek için büyük veri analitiğini kullanarak verilerin otomatik olarak işlenmesini sağlayan teknolojiler geliştirmeli ve kullanmalıdır.
    - "Siber Güvenlik Bakanlığı" kurulmalıdır.

- Dışişleri Bakanlığı içerisinde bir “Siber Büyükelçilik” kurulmalıdır. Siber krizlerin diplomasi yoluyla çözülmesi amacıyla çalışacak siber vatanın korunmasında diplomasi işletecek bir birim olmalıdır.
- İstihbarat kanununda değişikliğe gidilerek; terörizmi, casusluğu ya da şiddeti içeren aşırılığı finanse ettiğinden şüphelenilen kişi ve şirketlerin tüm bankacılık hareketleri izlenilebilmeli ve önlemler alınmalıdır.
- Yanıltıcı bilgilerin uygunsuz etkilerini belirlemek, analiz etmek, önleyebilmek ve yanıt vermek için bir Psikolojik Savunma Birimi kurulmalıdır.
- Siber güvenliğin Milli Siber Güvenliğin yanında ekonomik güvenliğinde önemli bir bileşeni olduğunu kabul edip, tedbirler alınmalıdır.

22. Ülkemizde kabul gören ve farkındalığımızı artıran “Siber Vatan” olgusu genişletilmeli, ülkemiz “Türk Dünyası Siber Vatan” olgusunu geliştirme de önderlik etmelidir.
23. Kuantum teknolojilerinin hızlı gelişimi dünya da endişeli alanlardan birisidir. Uluslararası işbirliği ile küresel siber güvenlik anlaşmalarının yapılacağı, kuantum güvenliğinin artırılması için ortak çabaların yoğunlaşacağı bir dönemin eşiğindeyiz. Kuantum anahtar dağıtımının, finansal işlemler ve yüksek güvenlikli veri iletimlerinde standart yöntem haline geleceği gerçeği gözardı edilmemelidir. Kuantum tehdidine karşı dirençli bir siber güvenlik ekosistemi kurulmuş olacağından bu döneme hazırlıklı olmak gereklidir. Kritik altyapıların güvenliğini sağlamak adına ulusal ve uluslararası işbirliklerinin artırılması, mevcut kriptografik sistemlerin kuantum sonrası dünyaya uygun hale getirilmesi ve araştırma-geliştirme çalışmalarının hızlandırılması çağrısında bulunuyoruz.
24. **Siber dayanıklılık**, **siber güvenlik**, **dijital egemenlik** ve **yapay zekâ uygulamaları** konularına odaklanan bu konferansta, Türkiye’nin bu alanlarda attığı adımların yanı sıra küresel çapta öne çıkan siber güvenlik uygulamaları ve gelecekte karşılaşılacak risklerin büyüklüğü dikkate alındığında, ulusal güvenlik için büyük dil modelleri geliştirilmeli ve kullanıma açılmalıdır. Özellikle de ülkemize ve dilimize özel büyük dil modelleri ve genel yapay zekâ uygulamaları geliştirilmeli ve genel kullanıma açılmalıdır.
25. Uluslararası sertifikasyonlara sahip Yerli milli ürünler ile dışa bağımlılığının azaltılması, siber saldırılara karşı güvenlik önlemlerinin yapay zeka destekli artırılması büyük önem arz etmektedir. Ancak yerli ve milli ürünlerin sürdürülebilirliğinin sağlanması, bu ürünlerin gelişimi açısından çok önemli olduğundan bu alanlar özel olarak desteklenmelidir.

26. Kuantum sonrası kriptografi için sunulan anahtar değişimi standartları belli bir olgunluğa ulaşmış ve gündelik uygulamalarda kullanılmaya başlanmıştır. Fakat kuantum bilgisayarlarına dayanıklı imzalama algoritmalarının hedeflenen güvenliği ve performansı sunabilmesi için aktif çalışmaların devam etmesi gerekmektedir. Hedeflenen özelliklerdeki kuantum sonrası algoritmalar bir gün standartlaşsa bile, siber güvenlik içim bu algoritmaların TLS ve DNSsec benzeri protokollerde nasıl kullanılacağı üzerine tartışılmalı ve araştırma yapılmalıdır. Yakın zamanda büyük çaplı bir kuantum bilgisayarın yapılması ve mevcut asimetrik kriptografi algoritmalarını kırması beklenmese de, bugün kaydedilen şifreli görüşmeler, on yıllar sonra böyle bir kuantum bilgisayarın icat edilmesi sayesinde dinlenebilir hale gelecektir. Bu nedenle bazı ülkelerin hedeflediği gibi Türkiye de 2030-2040 yıllarını kuantum sonrası kriptografik algoritmalara geçişi hedeflemeli, buna uygun altyapılar, test merkezleri, yazılım ve donanımların geliştirilmesi gibi konulara ağırlık vermelidir.

Kamuoyuna saygı ile duyurulur.

Bilgi Güvenliği Derneği
ISCTürkiye 2024 Düzenleme Kurulu